UNCLASSIFIED

# Defense Technical Information Center
# Compilation Part Notice

# ADP010660

TITLE: The COTS it Circle

DISTRIBUTION: Approved for public release, distribution unlimited

## This paper is part of the following report:

TITLE: Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS" [l'Utilisation des produits vendus sur etageres dans les applications militaires de defense "l'Exploitation sans merci des produits commerciaux"]

To order the complete compilation report, use: ADA389447

The component part is provided here to allow users access to individually authored sections of proceedings, annals, symposia, ect. However, the component should be considered within the context of the overall compilation report and not as a stand-alone technical report.

The following component part numbers comprise the compilation report:

ADP010659 thru ADP010682

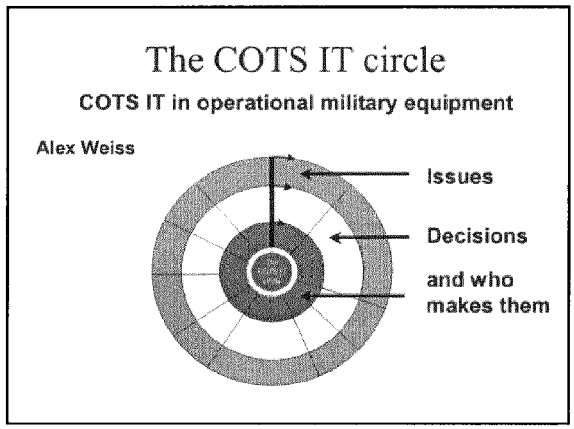
UNCLASSIFIED

# The COTS IT Circle

**Alex Weiss,**
**Defence Engineering Group, Department of Mechanical Engineering,**
**University College London,**
**4th floor, 66-72 Gower St, London, WC1E 6BT, United Kingdom.**
**e-mail a.weiss@ucl.ac.uk**

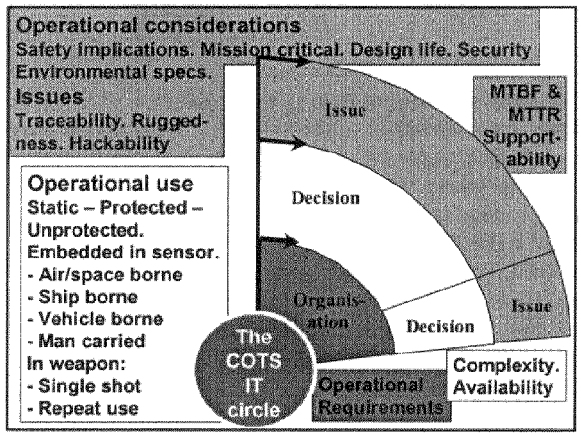
*An examination of the issues raised by using COTS IT in operational military equipment, the decisions that need to be made and who has to make them.*

The COTS IT Circle shows the issues raised when using COTS IT in operational military equipment. It looks at the decisions to be made and shows who has to make them. It starts by examining the main operational issues.




## Operational considerations

There are a number of operational factors that need to be considered at the start of any project. Four of them are particularly relevant to the utilisation of COTS IT.




### *Safety implications*

Does the use of the equipment have any safety implications and is it classified as a safety critical system? Such criteria demand the provision of a safety case; something that is difficult with a COTS IT-based system. Traceability is one of the key factors missing from virtually all COTS IT and there is little indication from the main suppliers that this situation is likely to change.

### *Mission critical*

While the equipment may not have a safety role, it may well be critical to the completion of its mission. Such roles include COTS IT embedded in key sensors and weapons. Clearly, duplication of low-reliability parts rapidly increases the chances of successful functioning throughout any mission.

### *Total design life*

The length of the design life of almost any piece of military equipment is far longer than for most of its civilian counterparts. A few aircraft and ships may remain in service, after a mid-life update, for as long as fifty years and a period of twenty-five years is commonplace. COTS IT, on the other hand, is obsolescent in eighteen months, obsolete in three years and mostly replaced within four years, even by the most cost-conscious users.

### *Interoperability*

Interoperability mainly revolves around the question of standards and in the case of COTS IT, these are largely de-facto standards. However, experience with popular programs such as Microsoft Office shows the difficulty of interoperability between different versions of the same programme. The problem may become significantly harder and more expensive to deal with when upgraded COTS software has to interface to custom military hardware with an interface to the original version of the COTS software.

## Operational use

The type of operational use will affect the type of requirements facing any COTS IT used. Almost all military equipment may experience a wide range of different environments depending on the particular application.

While, historically, defence specifications have carefully defined these different environments, COTS IT has had less care taken in specifying the environment in which it is to be used and suppliers to the military have made extensive use of wrapping to protect what would otherwise be very vulnerable items. The main area of COTS hardware differentiation has been between portable battery-powered items and mains-powered static ones.

### *Static*

By far the most benign environment is that which is static and protected. Examples include COTS IT installed in permanent defence ministry buildings and in headquarters bunkers. More demanding is the use equipment in a static but unprotected environment. These are increasing found when the armed forces are deployed overseas and will locate equipment in existing

*Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.*

buildings that may or may not have central heating, air conditioning or sealing from damp, dirt and dust.

***Embedded in sensor***

Sensors themselves may require some or a great deal of IT to function successfully. At the top end are the requirements of electronic warfare sensors, while at the bottom end are relatively simple sensors such are thermal imagers. The embedding may well take the form of wrapping, but consideration also needs to be given to the likely deployment of the sensor. Big air defence radars are unlikely to be moved, while a sonar buoy may have to withstand impact with the sea when dropped by an aircraft, not to mention exposure to the maritime environment.

***Air/space borne***

The nature of the unprotected environment in aircraft is severe. Low temperatures and pressures are often allied to high vibration and 'g' levels. There is, however, increasing pressure on the aerospace industry to provide pressurised, temperature-controlled compartments for avionics equipment, which is then mounted on suitable anti-vibration mounts.

The situation in spacecraft can be even more severe. Not only must the equipment survive the launch, but it must also cope with the wide range of temperatures, vacuum conditions, micrometeorite impacts and various types of radiation found in space.

In both cases, weight and volume are major considerations as are heat generation and power consumption; the last particularly in space applications. Furthermore, in aircraft, the production of poisonous fumes in the case of fire in the air must be avoided for the safety of the crew.

***Ship borne***

Areas of problem for COTS IT arise on board ships and submarines for a variety of reasons. The first is the presence of a salt-laden environment. Low frequency of vibration is a particular issue and equipment must be able to survive exceptional levels of shock should the vessel be hit by enemy action. The generation of smoke or poisonous fumes must be avoided, particularly in the case of submarines. While power consumption is less of an issue than in aircraft, the generation of excess heat below decks often calls for a water-cooled heat exchanger. A particular issue is the need for mission availability, which can be for 90 days or more, relying only on on-board support for maintenance.

***Vehicle borne***

Any equipment installed in a vehicle leads a tough life. Exposed to the ravages of the weather, it is also expected to survive very high levels of shock and vibration. Maintenance also usually takes place in a less than ideal environment.

***Man carried***

Any man-portable equipment has to survive a large degree of rough and tumble, particularly in wartime. The elements, dust and mud, being dropped or thrown into a vehicle are all the lot of man-portable equipment. Size, weight, silent operation and low power consumption are important issues.

***In weapons***

Weapons include guns, rockets, guided missiles, mines and torpedoes. Almost all experience serious stresses at launch.

***Single shot***

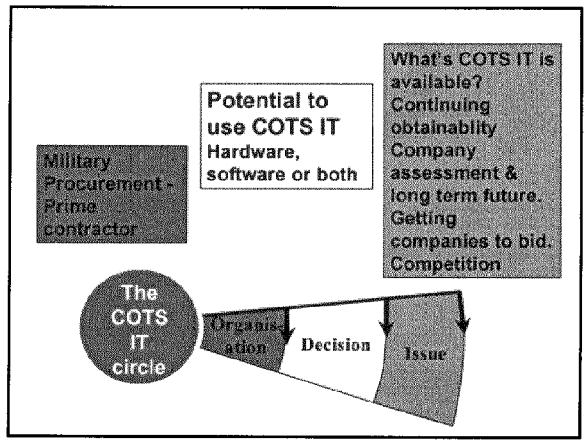
Any single-shot equipment must operate the first and only time that it is used after a storage period that may last for decades. The increasing trend towards 'sealed' rounds avoids any checking or maintenance.

***Repeat use***

The repeated shock on any item of equipment that is part of a multiple-firing weapon system is bound to be severe.

**What COTS IT is available**

People working in defence ministries and for defence contractors are finding it increasingly difficult to keep up to date with what is being offered in the market place. The main reason for this is that the range of products is increasing rapidly as the market grows and this is allied to speedy product obsolescence; the result of the rapid changes in technology.




**Company assessment & long term future**

Many commercial IT companies are both young and small in size. Some like Microsoft are enormous, yet still relatively young. Most are following the industry norm and growing very fast. Few are located just in a single country and it is commonplace for the larger companies to sub-contract work to employees in countries like Russia and China. This implies that either a defence ministry or its prime contractors must manage these predominantly overseas suppliers, with the risk that support may be embargoed in times of tension or war. As for the long-term future, who in 1980 would have predicted the fall from the top spot of IBM?

**Getting companies to bid**

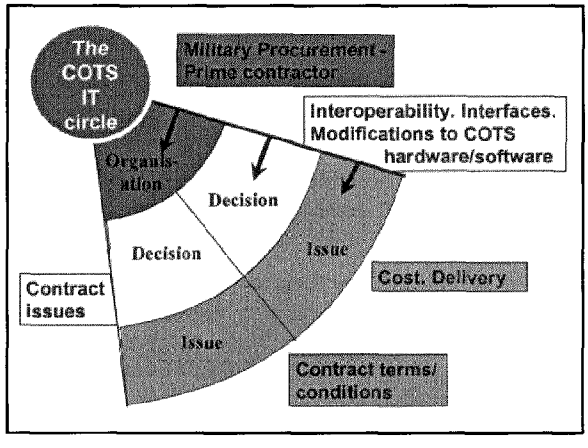
The commercial IT market is huge while the military IT market is very small; representing only one percent of the total. This, in itself, is not a great incentive for commercial companies to bid for military work. The attractions of bidding are further reduced by the

aggravation involved in the bidding and contracting hurdles put in place by government military purchasers.

**Competition**
There are monopolies, or near monopolies in some areas, and the dominance of Microsoft and Intel in the software and microprocessor markets is well established. This can mean that it is sometimes hard to find true competition and this gets worse, once a project is locked into a particular IT solution. In the case of hardware, there is a plethora of 'IBM PCs' but the performances of these look-alikes is by no means the same. Nor are they necessarily always suitable in terms of form, fit and function.

**Continuing obtain ability**
In the time from deciding the content of a tender to the award of a contract, an item of COTS IT hardware or software may no longer be available. A year is a long time in the commercial IT industry, but only a short time in the military acquisition process, the more so if platform (ship, tank or aircraft) time scales are taken into account. It may well be that the COTS item can only be obtained as an upgraded version, which may or may not meet the requirement. It is difficult to keep up to date in terms of knowing what COTS IT is on the market and matching this against what will be needed. For some military requirements, 'Milspec' equivalents will be essential and COTS IT may not be able to be wrapped or otherwise modified to meet these requirements. In these cases, it will be essential to fund specifically these military areas of IT.

**Potential to use COTS IT**
It is at the earliest stage that a decision must be made on the possibility of using COTS IT. Such a decision is likely to impact back into the equipment specification, which must reflect its proposed use.




**Delivery**
The delivery time of COTS IT is remarkably short. It may often be literally off-the-shelf and may, in any case, be too quick for the purchaser. On the other hand, it may no longer be available when required. Continuity of supply and build standard are both issues that cannot easily be resolved. Furthermore, once the COTS IT has been delivered, there may be significant system integration problems, both in terms of the need to protect hardware, and in both hardware and software interfacing.

**Cost**
There is no doubt that bespoke systems are now largely unaffordable from the current levels of defence equipment budget of the industrialised nations. There is a significant cost of testing COTS IT to prove that it is 'problem free', and this may need to be added to the actual purchase price. It should be noted that the US DoD is carry out a great deal of COTS IT testing at its own expense.

The life cycle cost implications of using COTS IT are largely unknown because no major platform or system has had time to pass through more than a fraction of its life since COTS IT started to be used.

Competitive policy tends to be anti-COTS IT, since once a particular supplier of, for example, some software has been chosen, that supplier will be the sole potential supplier of software upgrades.

***Modifications***
COTS IT is available at remarkably low prices for standard items, though these low costs rise to ridiculous levels if modifications are demanded. It is clear that the initial operational requirement must reflect the potential for COTS IT use if major modifications to standard items are to be avoided.

***Interoperability and interfaces***
The need for interoperability between different COTS IT-based equipment and between COTS IT-based and bespoke military equipment is largely an issue of cost. Careful though about the use of interfaces early in any programme is key to minimising costs at later stages.

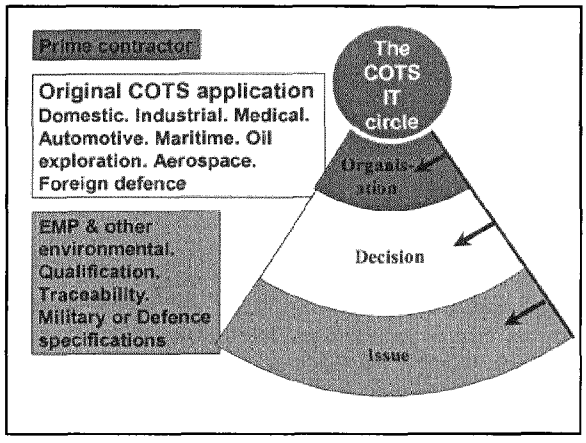
**Contract terms and conditions**

The terms and conditions of contract offered by defence ministries are not attractive and are often unacceptable to COTS IT suppliers; and this is particularly true of IPR. With most COTS IT suppliers located in the US or Pacific Rim, these firms are usually reluctant to send a negotiating team to another country for what they see as a contract in an irrelevant or sidelined market. Defence prime contractors are in no position to flow down their customer's terms and conditions to commercial IT companies and face a 'take it on our terms or leave it' attitude. Alternatives are to buy or licence software.

**Original COTS application**
It is clear that COTS IT is produced to many different standards, depending largely on the original application. A number of different commercial sectors are considered to examine how they vary.

***Domestic***
Equipment designed for use in the home, such as the microprocessors and other integrated circuits found in washing machines, microwave ovens and video recorders operates in a relatively benign environment. It is usually static, with a narrow operating temperature range. Electro-magnetic compatibility is important but design life for all white goods is only five years. Mobile

products, such as digital and video cameras are pushing a trend towards increasing physical robustness.




***Commercial***

Information technology designed for commercial use operates in a similar environment to domestic equipment but is usually required to be more reliable as the consequences of failure, for any reason, usually have financial implications. In addition, the consequences of a hacker accessing, for example, a banking or other financial system can be extremely serious. Anything from a PC-based system, through a server to a mainframe system may be crucial to the operation of any commercial concern.

***Industrial***

Industrial systems, particularly those operating on a continuous basis, such as production-line equipment in a steel or glass works, or those undertaking robotic tasks, must have the highest availability. Again, the environment can be remarkably demanding and wrapping of delicate electronic equipment is widespread.

***Medical***

Information technology may just be commercial or industrial adapted for a medical role but it may operate equipment, such as X ray machines, where incorrect operation has the capacity to kill. Thus some applications involve safety critical operations; a fact which may be particularly applicable to some military requirements.

***Oil Exploration***

Many of the areas where oil companies are exploring for new finds have hostile environmental conditions. These include rigs in the North Sea, South Atlantic and Gulf of Mexico, land-based equipment in Alaska and Siberia, as well as tropical and desert regions. The application of IT in this industry has provided some exceptional wrapping issues, with a salt-laden atmosphere common and extremes of temperature as wide as any experienced by military equipment.

***Nuclear***

Much of the IT equipment operating in the nuclear industry is actually used to control or monitor the operation of nuclear reactors. This is a very safety critical function and equipment failures or crashes cannot be tolerated. Historically, custom-built systems were the norm but, as with military IT, the nuclear industry is being forced to embrace COTS IT.

***Automotive***

Not only are some automotive applications of IT safety critical, such as drive by wire, but the equipment also has to operate in tough environment. A wide range of operating and survival temperatures and humidities is essential and the mobile environment implies a high level of shock and vibration. Engine management systems are often fitted close to high-revving internal combustion engines and must operate reliably through the design life of the vehicle – typically ten years. Much of the standard IT used on commercial vehicles is already being applied to military versions as well as to new military vehicles.

***Maritime***

In some ways more benign that the automotive environment, the salt atmosphere and low frequency vibration levels must be survived. Some systems again are safety critical, particularly those that control the engines and steering, while others, such as navigation systems may be mission critical. With long periods spent at sea, the only maintenance possible is that which the ship's engineering staff can carry out using on board spares.

***Aerospace***

The ultimate safety critical environment, civil flight control systems have to survive a pretty tough environment, in many ways similar to that found in military aircraft. These and other IT based systems can be exposed to trying conditions including a very wide range of temperatures, low pressures and a broad span of vibration and humidity.

Spacecraft, while less safety critical, have exposure to a wide range of severe environmental conditions both during launch and in the hostile emptiness of space itself. Furthermore, the cost of getting a satellite into Earth orbit or beyond is extremely expensive, making reliable performance a key criterion.

***Foreign defence***

Military equipment supplied to other nation's armed forces and then purchased off-the-shelf is different from normal COTS IT and is not considered further.

**Military or defence specification requirements**

COTS IT does not meet defence specification such as US mil specs and, worse, there is no audit trail. However, the specifications that COTS IT can meet are:

Increasingly severe.
Usually not guaranteed by the supplier.
Often better than the supplier suggests.

***EMP and other environmental***

Hardware is not radiation hardened and for many military applications, ruggedness still an issue, leading to the need for wrapping to provide the required level of protection. While environmental requirements in the commercial sector are increasing, and much COTS IT is built to avoid RFI, there is little actual testing and there

are no Tempest-proof items. Fire in a confined space, such as on board a submarine, could be worsened by the toxic products of combustion from some of the plastics and batteries found in COTS IT. However, there is convergence as commercial environmental specifications toughen and military ones relax.

**Qualification**
Qualification may be as fit for purpose, mission critical or safety critical. This requires testing to prove usability, environmental survival, reliability, maintainability and types of failure mode.

**Traceability**
While military equipment is normally traceable, in the sense that each part and each work package is carefully referenced, by and large such traceability does no exist in COTS IT products. Thus, where safety is an issue, it is difficult to provide proven safety cases.

It is noticeable, however, that certain industries are now converging on this military requirement and demanding traceability from the component suppliers and sub-contractors. Typical is the vehicle industry, which needs to know which particular vehicles to recall for safety checks. Much of this change is being driven by litigation concerns and is likely to apply increasingly to COTS IT, particularly hardware.

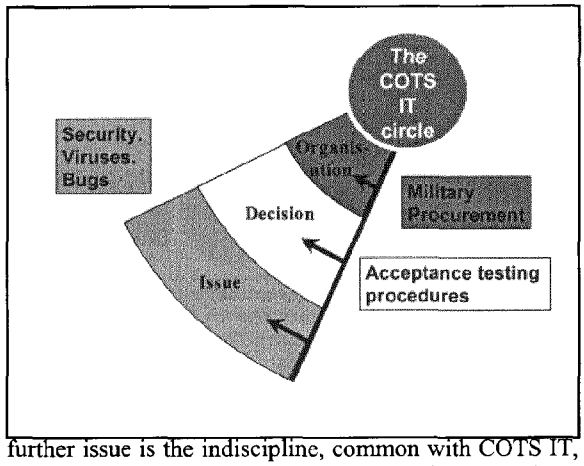
**Reliability**
COTS software is notoriously unreliable and prone to regular crashes, although it may well be better than certified custom military software of similar complexity. There is no database of failures and no traceable records for COTS IT, though the wide user base of much software does provide a degree of confidence. At the same time, there are problems with product liability and virtually valueless warranties for software. As mentioned earlier, the US DoD does prove COTS IT by both board and equipment level testing.

Acceptable MTBF and MTTR are key issues normally considered in the very early stages of the procurement cycle. The actual figures required will depend on a number of issues including the operational role, the operational environment, the consequences of failures and the ease of maintenance.

**Security**
The requirements of military security are currently different from commercial requirements, though the latter are being driven by the need for financial transaction security. Unfortunately, interfacing military crypto requires modification to standard COTS software and re-modification each time the software is upgraded.

The greatest problem lies with transmissions to and from platforms, where radio links are essential and can be intercepted. Commercial crypto usually takes several years to get accredited for military use and is, of course, also available to potential enemies.

***Hackability***
Designers leave built in trap doors in their software to allow future access. Hackers familiar with COTS software may readily exploit these entry points. A further issue is the indiscipline, common with COTS IT, in the use of passwords, a trend that has been accelerating with the increasing number of passwords and pin numbers that each individual has to remember.



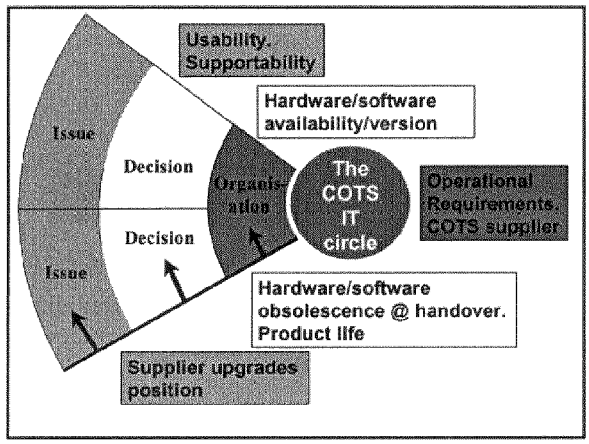

**Viruses**
One or more viruses may already be resident in COTS IT software, while world familiarity eases its infection and requires care to avoid providing entry points for viruses during the life of the equipment. In general, viruses written to work in custom military software are only likely to be generated by professionals employed by potentially hostile nations.

**Bugs**
All software contains bugs. These may occur at different frequencies and with different impacts on the user. There are bugs that may occur daily, weekly, monthly, yearly, once a decade or even once in an equipment's lifetime. One of the major difficulties is testing for bugs and in this area, COTS IT fairs well with large numbers of Beta testers, not to mention the often-large installed base. However, removing bugs has the unfortunate habit of introducing new ones, so that it may well be better to live with a number of bugs if their consequences are not severe.

**Supplier upgrade position**
No COTS IT supplier can continue to offer a standard product in the market place for very long without upgrading it. There are a number of drivers for this approach:

- Competition from other suppliers.
- Inadequacies in the existing product.
- The need to broaden the capabilities of the existing product.
- For software suppliers, to take advantage of improvements in hardware speed and memory.
- For hardware suppliers, to benefit from improvements in component and sub-system technology.

The result is that improved hardware comes on the market in a matter of months, while upgrades to software appear every one to two years.




**Usability and supportability**

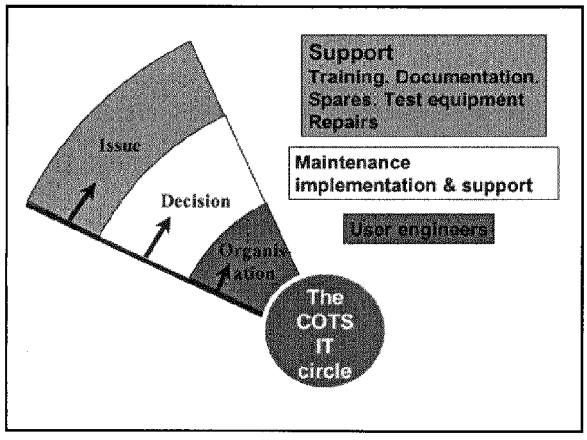
The general familiarity of people with COTS IT helps usability as does competition in the market place. Supportability usually depends primarily on the degree of obsolescence when the equipment is handed over to the user. Because of short COTS IT product lives, supportability will often depend on the prime contractor leaving the actual choice of COTS hardware and software as late as possible in the delivery programme.

***Rapid obsolescence***

Two years seems to be the time span before the issue of a major software upgrade for any particular program. From that point on, the older version ceases to be supported. The appearance of new hardware models is measured in months rather than years. Thus, the use of COTS IT forces the upgrade route on the purchaser when the supplier ceases support. Consideration should be given to upgrading only that hardware necessary to support new software needs.

**Support**

The term support is used here as the activities needed to enable equipment to be kept available for operational use. It includes training and provision of documentation for users and maintenance staff, as well as the supply of spares and test equipment.




***Training***

On the whole, COTS IT suppliers do not provide training in their products. This task is largely left to established training companies and can sensibly be incorporated in the equipment prime contract.

***Documentation***

COTS IT documentation is very thin, the choice of all suppliers being to provide the vast bulk of the information on CD ROMs. This format may change as DVDs and other new media replace CD ROMs. Some software programs also provide on-line support for registered users, allowing them to downloaded updates from supplier web sites. All this help may be printed out, but it is in the form of very basic word processing pages, largely without illustrations, rather than the excellent standard of most custom (and hideously expensive) military handbooks.

***Spares and test equipment***

Much COTS IT hardware is not designed for repair and thus spares support is limited both in extent and duration. In the commercial market, failed hardware is normally discarded if it fails outside the extended warranty period – normally three years. In any case, manufacturers' warranty repairs are likely to be of a form fit and function nature, where the failed unit may simply be replaced rather than repaired.

Much COTS IT hardware includes diagnostic software to facilitate faultfinding.

***Repairs***

The support of COTS IT demands a different maintenance policy to that in place for existing military equipment. COTS IT hardware is relatively reliable and, in the event of a failure, much of it is designed to be thrown away rather than repaired. Spares at board level are available only for a short period for current products and are not NATO codified. Both repair work and IT training have been largely sub-contracted by the IT industry. Whether, in these circumstances, prime contractors can provide long-term logistic support remains to be seen.

**Modifications and half life updates**

***Modifications***

Contractors are very reluctant to undertake modification to in-service COTS IT, and government financiers are somewhat reluctant to accept the standard upgrade process. There is a need for transparent interfaces and architecture at the start of any COTS IT-based programme to support future growth. Furthermore, any modification may introduce new bugs.

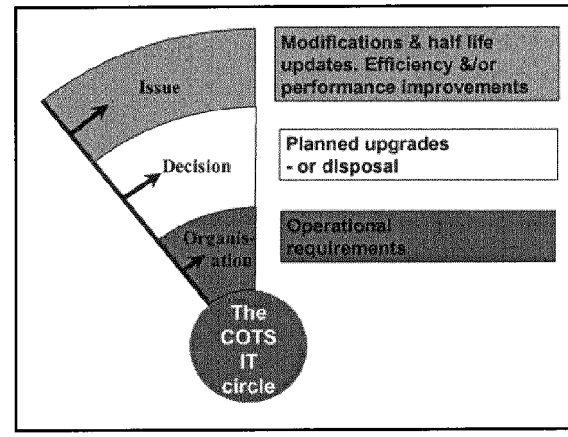
**Performance and efficiency improvements**

There are two main purposes for using any IT. The first is to improve ways of undertaking tasks to provide improved performance. The second is to do the task more efficiently. The fact that the equipment contains COTS rather than custom IT should not reflect on this issue. Efficiency improvements can be obtained by using, for example, a standard COTS human-machine

interface to avoid the need for retraining operators before they move to a new role.

**Disposal**

The decision to dispose of a piece of COTS IT is generally straightforward. However, care must be taken to ensure that any classified data are entirely and effectively removed from any storage medium, such as floppy and hard disks, CDs and tapes. Special care must then be taken with their declassification or destruction.



# The COTS IT Circle helps identify issues, the decision that must be made and who has to make them, when using COTS IT in military equipment

Abbreviations
**MTBF** – Mean time between failures
**MTTR** – Mean time to repair
**IPR** – Intellectual property rights

**DPA** – Defence Procurement Agency
**OR** – Operational Requirements